**Department of Technology & Information**
**Policy and Procedures Manual**
**Subject:** **Acceptable Use Policy**
**Purpose:** Guide Behaviors in Using the State's Communications and Computer Systems
**Effective Date:** April 15, 2003
**Approved by:** Thomas M. Jarrett

## A Message to all System Users

This document formalizes the State policy for state agency and public school district employees as well as contractors and other "users" of our State's communications and computer systems. Each agency/school district or affiliate may also choose to develop and enforce its own acceptable use policies to further restrict the use within its local environment. This may be done only with the understanding that, should a conflict exist, the State's Acceptable Use Policy takes precedence over all local policies developed within the agencies/affiliates for the explicit purpose of exercising responsible controls at the local level.

Our goal is to put controls in place that will help protect the State from sabotage and espionage. The threat is real, as each month, DTI intercepts tens of thousands of viruses and suspicious messages containing executable files trying to bypass our security systems. These controls also help minimize the potential risks of misuse. This misuse includes unnecessary Internet usage causing network and server congestion. This Acceptable Use Policy is your (the user's) guide for helping us achieve this goal by conducting State of Delaware business with integrity, respect, and prudent judgment. Each of us is responsible for upholding the State's commitment to the highest standards of conduct.

***Affiliates include the Judicial Branch, the Legislative Branch, and other State & Local government political sub-divisions authorized to use these state services.***

**Users are accountable** for familiarizing themselves with this policy and using it as a guidepost for your daily decisions and actions when using these services.

Each agency/school district and affiliate organization(s) are responsible for the activity of its users and for ensuring that its users follow this Acceptable Use Policy. Violations, which are not promptly remedied by the client organization, may result in termination of these services.

***Secretary Thomas M. Jarrett - Chief Information Officer***

## Introduction

This Acceptable Use Policy is your resource to help you make sound decisions in using communications and computer systems to do your job.
**All of us have a responsibility to**:
***Read:*** the policy and give careful attention to those subjects that most pertain to your job duties.
***Understand:*** the purpose of this policy and your overall responsibilities for standards of business conduct.
***Consult:*** your supervisor or organization's Information Resource Manager (IRM) for additional clarification of this policy.

Note the Following:

### *Applicability*

State of Delaware's expectations for responsible use are applicable to all parties who use the State communications and computer systems on behalf of the State, including, but not limited to, its agency, school district, and affiliate employees, consultants, in-house contractors, and other "users."

### *Limitations*

This acceptable use policy does not address every expectation or condition regarding acceptable use. It does not substitute for other more specific State policies and procedures.

### *Version*

This document contains corrections made 8/8/2005 to the link to DTI standards, reference to the correct section of the Merit rules, and name change for the Customer Relationship Specialist.

# Acceptable Use of Communications and Computer Systems

State of Delaware communications and computer systems are vital to our business and critical to overall communications. Our success is directly related to safeguarding and properly using these systems.

## WHAT ARE STATE COMMUNICATIONS AND COMPUTER SYSTEMS?

State of Delaware communications and computer systems are any equipment, hardware, software or networks (including wireless networks) owned, provided or used by or on behalf of State of Delaware that store or transmit voice or non-voice data. This includes telephones, cellular/wireless telephones, voice mail, computers, e-mail, facsimiles, pagers, and State Intranet or Internet access (including when accessed through personal computers).

***Note: When personal computers are not owned by the state but are used for State business, the State retains the right to access any State records or materials developed for State use. Also, we must ensure that any State materials are appropriately safeguarded according to applicable standards in this section, including, but not limited to, virus protection of, protected access to and backup of these materials.***

### *Access, Maintenance and Protection*

Users must safeguard the confidentiality and integrity of State systems, including strong password logons (*see Windows 2000 password criteria at the end of this document),* access codes, network access information, log-on IDs) from improper access, alteration, destruction and disclosure. Users shall only access or use these systems when authorized. Users must abide by State standards contained in this section and other State policies regarding protecting data and information stored on these systems. All DTI standards are available at http://intranet.state.de.us/dti.

### *Unlawful and Inappropriate Use*

Users are obligated to never use State systems (such as the Intranet or Internet) to engage in activities that are unlawful, violate State policies or in ways that would:

- Be disruptive, cause offense to others, or harm morale.
- Be considered harassing or discriminatory or create a hostile work environment.
- Result in State of Delaware's liability, embarrassment or loss of reputation.

External groups or organizations are not permitted to make announcements, solicitations or otherwise access the State's Communications and Computer Systems, except as permitted by law.

### *Protection and Integrity of Data*

Users must maintain the integrity of State Information and data stored on State systems by:

- Only introducing data into our systems that serves a legitimate business purpose.



- Only acquiring, using, altering, disposing of, or destroying data or information with proper authorization.
- Protecting data and information stored on or communicated across our systems and not accessing this data or information (for example, agency data, employee records) unless authorized.
- Protecting data and information communicated over internal or public networks (for example, the Internet) to avoid compromising or disclosing nonpublic State Information or communications.

### *Personal Use*

While State systems are intended for primarily business/instructional purposes, limited (incidental and occasional) personal use may be permissible when authorized by your management and it does not:

- Interfere with your work responsibilities or business/instructional operations.
- Involve interests in personal outside business and/or other non-authorized organizations and activities (which may include, but is not limited to selling personal property/items or soliciting for or promoting commercial ventures, charitable, religious or political activities or causes).
- Violate any of the standards contained in this code or other State of Delaware policies.
- Lead to inappropriate costs to the State. (Excessive personal surfing, utilizing streaming services such as listening to music or watching video, and downloading of music and video files are specifically forbidden.)

### *Virus Protection*

Users must check all electronic media, such as software, diskettes, CD-ROMs and files for viruses when acquired through public networks (for example, the Internet) or from outside parties using virus detection programs prior to installation or use. If users suspect a virus, they must not use the applicable computer systems and equipment until the virus is removed and they will report the matter immediately to the appropriate network security contact. The Department of Technology and Information has purchased anti-virus software for all government sites including home computers. Similarly the Delaware Center for Educational Technology has purchased anti-virus software for all public K-12 schools.

### *Properly Licensed Software*

Users will only use approved and properly licensed software and will use it according to the applicable software owner's license agreements.

### *Treatment of Third-Party Data or Software*

Users must ensure that any nonpublic State Information or software of a third party that is stored, copied, or otherwise used on State systems is treated according to State of Delaware's standards regarding nonpublic State Information and applicable agreements and intellectual property restrictions.

### *State of Delaware Monitoring*

State communications and computer systems, including, but not limited to, computer networks, data files, e-mail and voice mail, may be monitored and/or accessed by the State to ensure the integrity of the technology, protect against fraud and abuse, detect unauthorized access or use, and for other business purposes. Although the Department of Technology and Information (DTI) does not randomly monitor message or network transactions, DTI may without notification or approval, monitor, access and review any and all communications originating from the State of Delaware or delivered to the State of Delaware – employees should have no expectation of privacy in regard to use of these services. This is in accordance with 19 Del. C. chapter 7.

## USE OF EMAIL AND THE INTERNET

### Inappropriate use of e-mail includes, but is not limited to, sending or forwarding:

- Messages, including jokes or any language, that may be considered discriminatory, harassing, unlawful, defamatory, obscene, offensive, insensitive or otherwise inappropriate (this includes but is not limited to, messages about age, race, gender, disability, sexual orientation, national origin or similar matters).
- Pornographic or sexually explicit materials.
- Chain letters.
- Information related to religious materials, activities or causes, including inspirational messages.
- Charitable solicitations unless sanctioned by State of Delaware.
- Gambling.
- Auction-related information or materials unless sanctioned by State of Delaware.
- Games or other software or copyrighted materials without a legitimate business or instructional purpose (and then only according to the rights and licenses granted by the owner of the games, software or copyrighted material).
- Messages that disparage other companies or products.
- Large personal files containing graphics materials or audio files (such as photographs and music).
- Materials related to personal commercial ventures or solicitations for personal gain (for example, messages that could be considered pyramid schemes).
- Information related to political materials, activities or causes unless sanctioned or permitted by the State of Delaware.
- Unauthorized or inappropriate mass distribution of communication.
- Any other materials that would be improper under this policy or other State of Delaware policies.

### Inappropriate use of the Internet includes, but is not limited to, accessing, sending or forwarding information about, or downloading (from):

- Sexually explicit, harassing or pornographic sites.
- “Hate sites” or sites that can be considered offensive or insensitive.
- Auction or gambling sites.
- Non State of Delaware business-related chat sites.
- Underground or other security sites which contain malicious software and/or instructions for compromising State of Delaware security.
- Games, software, audio, video or other materials that we are not licensed or legally permitted to use or transmit or that are inappropriate, or not required by, State of Delaware business or instruction.
- Offensive or insensitive materials, such as sexually or racially oriented topics.
- Any other materials that would be improper under this policy or other State of Delaware policies.

### Inappropriate use of the Internet also includes:

- Intentional importation of viruses.
- Registering Internet domain names of the State of Delaware business/school district or those of third parties without authorization from DTI.

***Note: In order to perform their job duties (for example, network monitoring), specific State of Delaware employees may receive management approval exempting them from some of the above restrictions.***

## REMEDIAL ACTION

When DTI learns of a possible inappropriate use, DTI will immediately notify the agency/school district or affiliate responsible, which must take immediate remedial action and inform DTI of its action. In instances where agencies/school districts or affiliates do not respond in a timely or reasonably appropriate manner, are "repeat offenders", or if criminal activity is suspected, DTI will work directly with the proper authorities, and follow their guidance in determining appropriate action.

***Any inappropriate use of State communications and computer systems may be grounds for discipline up to and including dismissal based on the just cause standard set forth by Merit Rules, or collective bargaining agreement, whichever is applicable to the subject employee. Exempt employees shall be subject to appropriate discipline without recourse, except as provided by law.***

In an emergency, in order to prevent further possible unauthorized activity, DTI may temporarily disconnect that agency or affiliate. If this is deemed necessary by DTI staff, every effort will be made to inform the agency or affiliate prior to disconnection, and every effort will be made to reestablish the connection as soon as it is mutually agreed upon.

Any determination of non-acceptable usage serious enough to require disconnection will be promptly communicated to the Senior Manager at the agency or affiliate by the DTI Executive Team.

Unauthorized activity or non-acceptable usage determined at the agency/school district or affiliate may be subject to remedial action being taken in accordance with the acceptable use policy of that agency/school district or affiliate as well as those actions outlined above. The remedial action outlined in agency/school district or affiliate policies may differ from the remedial action as outlined in this policy.

DTI provides access to state, national and international resources to its clients through connections with networks outside of Delaware. In general, it is the responsibility of those networks to enforce their own acceptable use policies. DTI will make every attempt to inform its clients of any restrictions on use of networks to which it is directly connected; as such information is made available by the network provider.

DTI accepts no responsibility for traffic that violates the acceptable use policy of any directly or indirectly connected networks beyond informing the client that they are in violation if the connected network so informs DTI.

## QUESTIONS OR COMMENTS ON THIS POLICY

1. Users should offer comments or seek clarification through their supervisor or Agency/School District or Affiliate IRM.

2. Agency/School District or Affiliate IRM's should offer comments or seek clarification using one of the methods below:
    a. Your assigned DTI Customer Relationship Specialist (preferred) or
    b. E-mail to: colleen.gause@state.de.us
    c. Fax: 302-739-9642 , Attn. Colleen Gause
    d. Mail: Department of Technology and Information, Wm. Penn Bldg., 801 Silver Lake Blvd., Dover, DE 19901

## WINDOWS 2000 PASSWORD CRITERIA

The State selected a password-based authentication scheme that makes compromises between what is convenient for the user and what is difficult to circumvent. As part of the Windows 2000 implementation, the State has deployed a strong password policy. As additional state agencies and affiliates are added to the windows 2000 environment, password management will be automatically managed via DTI. School districts, which manage their own password policy, should begin deploying strong passwords as they migrate from legacy operating systems to Window 2000. The guidelines for strong passwords are established by the SANS Institute and recommended by the Microsoft Corporation as well as the Department of Homeland Security Information Analysis & Infrastructure Group. These guidelines are consistent with the password policies at most major government facilities.

Strong passwords require the following characteristics:

✓ Be at least seven characters long.

✓ Passwords must contain characters from at least three (3) of the following four (4) classes:

| DESCRIPTION | EXAMPLES |
|---|---|
| English upper case letters | A, B, C, ... Z |
| English lower case letters | a, b, c, ... z |
| Westernized Arabic numerals | 0, 1, 2, ... 9 |
| Non-alphanumeric ("special characters") | #,$,%,& such as punctuation symbols etc. |

✓ Not contain your name or user name.

✓ Not be a common word or name.

Additional information concerning strong passwords is available at the DTI WEB Site:
http://intranet.state.de.us/dti/standards/strong_passwords.pdf

***Passwords can be the weakest link in a computer security scheme. Strong passwords are important because password cracking tools continue to improve and the computers used to crack passwords are more powerful. Network passwords that once took weeks to break can now be broken in hours.***

- The system will force a password change every 120 days.
- You will start getting daily reminders to change your password 14 days in advance of the expiration of your current password.
- Users experiencing password problems should contact the DTI Service Desk on 302-739-9560.

## ACKNOWLEDGMENT STATEMENT

# State Of Delaware
# Acceptable Use Policy
# April 15, 2003

This is to certify that I have read and agree to abide by the guidelines set forth within the State Acceptable Use Policy. As an employee or business partner of the State of Delaware, I fully intend to comply with this policy realizing that I am personally liable for intentional misuse or abuse of the State's communications and computer systems. If I have any questions about the policy, I understand that I need to ask my supervisor or IRM for clarification. Users are also encouraged to take and score 100% on the AUP self-test located on the DTI Intranet at:
http://intranet.state.de.us/dti/aup/State of Delaware AUPSelfTest.htm

***If I refuse to sign this acknowledgement form, my supervisor will be asked to sign this form indicating that I have been given time to read and have questions answered about this policy. The supervisor will read this statement to me prior to signing the document and advise me that by not signing this document my rights to use the State's Communications and Computer Systems may be denied and may affect my ability to meet my job requirements.***

Name:_____

Signature: _____

Agency/Company/School: _____

Date: _____

Supervisor Signature (*as required)_____

Comments: _____